REMARKS

Claims 1-69 and 71 were currently pending in the application. Claims 4 and 5 have been cancelled. Claims 1, 6, 10, 11, 12, 13, 46, 69 and 71 have been amended. Claims 72 and 73 have been added. Claims 1-3, 6-69, and 71-73 are pending in the application.

35 U.S.C. § 102 and § 103 Rejections:

Claims 1-35, 39-62, 66-69 and 71 were rejected under 35 U.S.C. § 102(b) as being anticipate by Beach, U.S. Patent Application Publication 2001/0055283. Claims 36-38 and 63-65 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Beach in view of Campbell, NPL, November 2000. Applicant respectfully traverses these rejections.

With respect to the § 102(b) rejection, **the cited reference fails to teach or suggest all of the elements of the independent claims.** The teachings of Beach were discussed in the previous office action response.

Independent claim 1 recites:

> "A method of performing encrypted WLAN (Wireless Local Area Network) communication, comprising the steps of:
>
> operating driver software to perform a connection set-up for said encrypted WLAN communication, wherein performing said connection set-up comprises exchanging cryptographic keys between a WLAN station and another WLAN station and/or a WLAN access point; and
>
> operating a WLAN chip to perform data frame encapsulation and/or decapsulation during said encrypted WLAN communication;

wherein said connection set-up is performed by executing software-implemented instructions of said driver software without exchanging intermediate data with said WLAN chip; and

wherein said data frame encapsulation and/or decapsulation is performed by operating single-purpose hardware of said WLAN chip without executing software-implemented instructions of said driver software, wherein performing said encrypted WLAN communication further comprises obtaining a plurality of data frames intended for said data frame encapsulation from driver software" (Emphasis added).

Independent claims 46, 69, and 71 recite similar combinations of features.

The standard for anticipation is one of strict identity. MPEP 2131 states: "A claim is anticipated only if each and every element as set forth in the claim is found, either **expressly** or **inherently** described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987) (emphasis added). Applicant respectfully submits that Beach fails to describe various ones of the elements recited in the independent claims, either expressly or inherently, and thus does not anticipate the claims.

In the present office action, the Examiner contends that Beach teaches, in paragraph [0094], the limitation of "wherein performing said connection set-up comprises exchanging cryptographic keys between a WLAN station and another WLAN station and/or a WLAN access point." Applicant respectfully disagrees. Paragraph [0094] of Beach states the following:

[0094] The WEP processing if performed in the RF port 50, is a harder function to perform than CRC-32 since it includes both an

RC4 encryption function and a second CRC-32. At the same time it does not need to be completed prior to ACK generation/reception nor is performed on every packet (just data packets). The RC4 encryption function consists of two parts: building the encryption table (a 256 byte table) using the selected key and doing the encryption/decryption process. Based on sample code, it is estimated that building the table would require about 1200 instructions (12 ms at 100 MIPS) and the encryption/decryption process would require about 12 instructions/byte. There is no difference in this cost for 40 or 128 bit keys. The WEP CRC-32 would require another 13 instructions per byte.

Nowhere in the above citation is there any teaching or suggestion of exchanging cryptographic keys between a WLAN station and another WLAN station, either during a connection setup or any other time. The above discussion simply relates to different types of encryption functions, but does not discuss the exchanging of cryptographic keys or performing a connection set-up. Thus, contrary to the Examiner's contention, the above citation does not teach or suggest, either expressly or inherently, the exchanging of cryptographic keys during a connection set-up, particularly in combination with a connection set-up that is "performed by executing software-implemented instructions of said driver software without exchanging intermediate data with said WLAN chip" as also recited in claim 1.

The Examiner further contends that "wherein said data **frame** encapsulation and/or decapsulation is performed by operating single-purpose hardware of said WLAN chip without executing software-implemented instructions of said driver software" is taught by Beach in paragraphs [0060]-[0062] and [0110]. Paragraphs [0060]-[0062] state:

[0060] Wired Equivalent Privacy encryption/decryption (WEP)

[0061] Fragmentation/Reassembly

[0062] Data Movement

Paragraph [0059], which refers to these functions, states:

> [0059] The following optional (higher or lower) level MAC functions can be placed in either the higher or lower level categories.

Thus, the functions listed in paragraph [0060]-[0062], according to the teachings of Beach, may, optionally, be higher level or lower level MAC functions.

In paragraph [0107], Breach states:

> [0107] The location of the upper level MAC functions may vary considerably. Some possibilities are:

while paragraph [0110], cited by the Examiner states:

> [0110] Roaming/association on host processor 22, rest on MAC engine 26.

However, none of these paragraphs, expressly or inherently, teach data frame encapsulation/decapsulation, much less data frame encapsulation performed by a single-purpose hardware of said WLAN chip. The above paragraphs merely list some functions and their locations, but no teaching, express or inherent, is made to data frame encapsulation/decapsulation, much less performing said data frame encapsulation/decapsulation using single-purpose hardware of the WLAN chip.

The Examiner further contends that Beach teaches the limitation "wherein performing said encrypted WLAN communication further comprises obtaining a plurality of data frames intended for said data frame encapsulation from driver software" as recited in combination with the other features of independent claim

1. As noted above, Beach fails to describe, either expressly or inherently, data frame encapsulation, and thus does not teach this combination of features. The Examiner cites Beach as paragraphs [0111], [0121], and [0131] as teaching this combination of features. Paragraph [0111] of Beach states:

> [0111] Roaming/association/retransmission on host 22, rest on MAC engine 26. The choice of the location of the higher level MAC functions has a major impact on the cost of MU WLAN adapter. If one is willing to place at least some of the higher level functions on a host processor 22, then one could get by with just the 5402 on the WLAN adapter. Possible functions to place on the host would be roaming and association control. Higher level functions such as retransmission and fragmentation/reassembly could be left on the 5402. This split would permit significant savings, since another processor/memory subsystem would not be needed on the WLAN adapter. There are two reasons for not placing all of the MAC functions on the 5402. The first is memory space on the 5402 is only 32 KB of SRAM for both code and data. In some MAC implementations such as frequency hop, the code space alone exceeds 32 KB. The second reason is that the software on the 5402 is oriented toward meeting hard, real-time tasks such as CRC and WEP processing. Trying to add software intensive tasks would only complicate the process.

The above paragraph discusses the location of higher level and lower level functions, but provides no description, either expressly or inherently, of data frame encapsulation, much less "obtaining a plurality of data frames intended for said data frame encapsulation from driver software" as recited in combination with the other features of claim 1.

Paragraph [0121] of Beach states:

[0121] The cell controller 14 includes applications to provide mobile unit association management, roaming and packet buffer management. These applications are similar to those performed by current access points in the Spectrum 24 system. The cell controller 14 may also provide QoS support, user authorization and configuration management. Placing these functions on a personal computer cell controller facilitates system management and program updates using available programming tools. Further, modifications to authorization or management functions need only be installed into the cell controller 14, and no modification to the software of the RF ports 18 is required.

The above paragraph discusses the location of certain functions, but provides no description, either expressly or inherently, of data frame encapsulation, much less "obtaining a plurality of data frames intended for said data frame encapsulation from driver software" as recited in combination with the other features of claim 1.

Paragraph [0131] of Beach states:

[0131] In the FIG. 7 example host 90 sends message "A" having 100 data bytes via an Ethernet packet 100 to cell controller 14. Packet 100 has a destination address of the Mobile unit (M1), a source address of the host (H) and includes data (A). Cell controller 14 formats the data in 802.11 format with the destination corresponding to mobile unit (MU1) 20. The cell encapsulates this 802.11 packet with data A into an Ethernet packet 104 addressed to RF port 1 (RF1) from the cell controller (CC).

The above paragraph discusses the sending messages and formatting data in 802.11 format, but provides no description, either expressly or inherently, of data

frame encapsulation, much less "obtaining a plurality of data frames intended for said data frame encapsulation **from driver software**" as recited in combination with the other features of claim 1.

For at least these reasons, Applicant submits that a case of anticipation has not been established. Accordingly, removal of the § 102(b) rejection is respectfully requested.

With regard to the § 103(a) rejection, Applicant notes that this rejection is directed to claims which depend from the independent claims discussed above, wherein Beach is relied upon as the primary reference. Accordingly, for at least the reasons stated above, Applicant submits that the prior art references, taken singly or in combination, fail to teach or suggest all of the elements of the independent claim. Applicant therefore respectfully requests removal of the 35 U.S.C. § 103(a) rejection.

Patentability of the Added Claims:

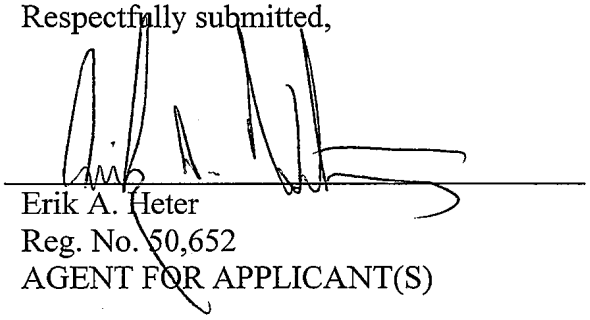
The present amendment adds claims 72 and 73. Claims 72 and 73 depend from claim 1. Applicant submits that no new matter has been added, and that the claims are fully supported in the specification (e.g., Fig. 4, page 9, line 26 to page 10, line 6). Applicant further submits that newly added claims 72 and 73 are patentably distinct from the cited art for at least the same reasons given above.

CONCLUSION

Applicant submits the application is in condition for allowance, and an early notice to that effect is requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5800-00601/EAH.

Respectfully submitted,



Erik A. Heter
Reg. No. 50,652
AGENT FOR APPLICANT(S)

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8800

Date: 11/14/07